

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-141816

(P2003-141816A)

(43) 公開日 平成15年 5月16日 (2003.5.16)

(51) Int.Cl. ⁷	識別記号	F I	テ-マ-ド [*] (参考)
G 1 1 B 20/10		G 1 1 B 20/10	H 5 B 0 1 7
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 B 5 C 0 5 2
H 0 4 L 9/16		H 0 4 N 5/76	Z 5 C 0 5 3
H 0 4 N 5/76		5/92	H 5 D 0 4 4
5/92		H 0 4 L 9/00	6 4 3 5 J 1 0 4
		審査請求 有	請求項の数20 O L (全 15 頁)

(21) 出願番号 特願2001-335419(P2001-335419)

(22) 出願日 平成13年10月31日 (2001. 10. 31)

(71) 出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72) 発明者 津曲 康史

神奈川県川崎市幸区柳町70番地 株式会社
東芝柳町事業所内

(72) 発明者 三村 英紀

神奈川県川崎市幸区柳町70番地 株式会社
東芝柳町事業所内

(74) 代理人 100058479

弁理士 鈴江 武彦 (外6名)

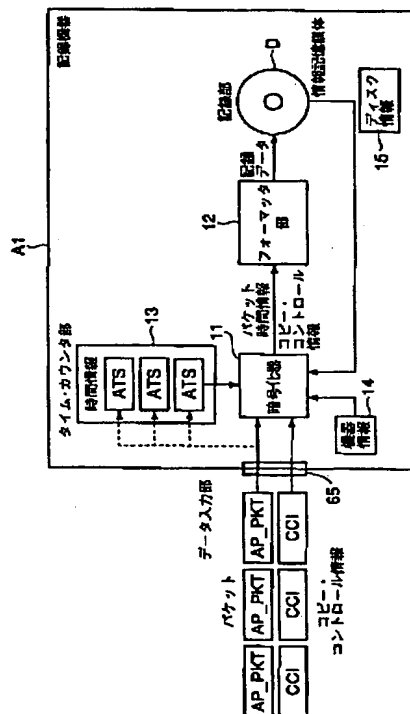
最終頁に続く

(54) 【発明の名称】 パケットデータの情報記録再生装置、情報記録媒体及び方法

(57) 【要約】

【課題】 パケットごとに異なる鍵情報で暗号化を行うことにより、高い解読困難性とアクセスの高速化を可能とする情報記録再生装置を提供する。

【解決手段】 パケットデータを単位として与えられる複数のパケットデータである所定情報を入力するインタフェース65と、入力された所定情報をパケットデータごとに異なる複数の鍵情報13を用いてそれぞれ暗号化する暗号化器11と、暗号化された暗号化所定情報をディスクDの記憶領域に記録するフォーマット部12とを有する情報記録装置であり、従来に比べより多くの鍵情報による暗号化を行うことで、一層のセキュリティの向上を図ることができる。



【特許請求の範囲】

【請求項1】 情報記録媒体に所定情報を記録する情報記録装置であって、

パケットデータを単位として与えられる複数のパケットデータである所定情報を入力する入力手段と、
前記入力手段が入力した所定情報を、パケットデータごとに異なる複数の鍵情報を用いてそれぞれ暗号化する暗号化手段と、

前記暗号化手段により暗号化された暗号化所定情報を、前記情報記録媒体の記憶領域に記録する記録手段と、
を具備することを特徴とする情報記録装置。

【請求項2】 前記複数の鍵情報は、各パケットデータが前記入力手段に到着した時間情報に基づくものであることを特徴とする請求項1記載の情報記録装置。

【請求項3】 前記複数の鍵情報は、各パケットデータが前記入力手段に到着した時間情報と、各パケットデータに含まれるヘッダ領域の少なくとも一部のデータとに基づくものであることを特徴とする請求項1記載の情報記録装置。

【請求項4】 前記複数の鍵情報は、各パケットデータの少なくとも一部のデータに基づくものであることを特徴とする請求項1記載の情報記録装置。

【請求項5】 前記複数の鍵情報は、各パケットデータが前記入力手段に到着した時間情報と、各パケットデータのペイロード部分の少なくとも一部とに基づくものであることを特徴とする請求項1記載の情報記録装置。

【請求項6】 前記記録手段は、前記暗号化手段により暗号化された暗号化所定情報を、各パケットデータがそれぞれ前記入力手段に到着した時間情報をそれぞれ伴って前記情報記録媒体の記憶領域に記録する手段を更に有することを特徴とする請求項1記載の情報記録装置。

【請求項7】 情報記録媒体に格納されている所定情報を再生する情報再生装置であって、
前記情報記録媒体の記憶領域に格納されているパケットデータ単位に暗号化された所定情報を読み出す読出手段と、
前記読出手段が読み出した前記所定情報を、パケットデータ単位に異なる複数の鍵情報を用いて復号化することにより再生する再生手段と、
を具備することを特徴とする情報再生装置。

【請求項8】 前記複数の鍵情報は、各パケットデータが暗号化された際に各パケットデータが暗号化装置に到着した各々の時間情報に基づくものであることを特徴とする請求項7記載の情報再生装置。

【請求項9】 前記複数の鍵情報は、各パケットデータが暗号化された際に各パケットデータが暗号化装置に到着した各々の時間情報と、各パケットデータに含まれるヘッダ領域の少なくとも一部のデータとに基づくものであることを特徴とする請求項7記載の情報再生装置。

【請求項10】 前記複数の鍵情報は、各パケットデー

タの少なくとも一部のデータに基づくものであることを特徴とする請求項7記載の情報再生装置。

【請求項11】 前記複数の鍵情報は、各パケットデータが暗号化された際に各パケットデータが暗号化装置に到着した各々の時間情報と、各パケットデータのペイロード部分の少なくとも一部とに基づくものであることを特徴とする請求項7記載の情報再生装置。

【請求項12】 前記読出手段は、前記暗号化手段により暗号化された暗号化所定情報と、各パケットデータが暗号化装置に到着した各々の時間情報とを、前記情報記録媒体の記憶領域から読み出す手段を更に有することを特徴とする請求項7記載の情報再生装置。

【請求項13】 所定情報を各パケットデータごとに暗号化されて格納する情報記録媒体であって、
パケットごとに異なる複数の鍵情報によりそれぞれ暗号化された複数の暗号化パケットデータを、記憶領域に格納していることを特徴とする情報記録媒体。

【請求項14】 前記複数の鍵情報は、各パケットデータが前記入力手段に到着した時間情報に基づくものであることを特徴とする請求項13記載の情報記録媒体。

【請求項15】 前記複数の鍵情報は、各パケットデータが、これらの各パケットデータの暗号化処理を行った暗号化装置に到着した時間情報と、各パケットデータに含まれるヘッダ領域の少なくとも一部のデータとに基づくものであることを特徴とする請求項13記載の情報記録媒体。

【請求項16】 前記複数の鍵情報は、各パケットデータの少なくとも一部のデータとに基づくものであることを特徴とする請求項13記載の情報記録媒体。

【請求項17】 前記複数の鍵情報は、各パケットデータが、これらの各パケットデータの暗号化処理を行った暗号化装置に到着した時間情報と、各パケットデータのペイロード部分の少なくとも一部とに基づくものであることを特徴とする請求項13記載の情報記録媒体。

【請求項18】 各パケットデータが前記入力手段に到着した各々の時間情報を、前記暗号化パケットデータの各々に伴って格納していることを特徴とする請求項13記載の情報記録媒体。

【請求項19】 情報記録媒体に所定情報を記録する情報記録方法であって、
パケットデータを単位として与えられる複数のパケットデータである所定情報を入力する入力工程と、
前記入力工程で入力した所定情報を、パケットデータごとに異なる複数の鍵情報を用いてそれぞれ暗号化する暗号化工程と、
前記暗号化工程により暗号化された暗号化所定情報を、前記情報記録媒体の記憶領域に記録する記録工程と、
を具備することを特徴とする情報記録方法。

【請求項20】 情報記録媒体に格納されている所定情報を再生する情報再生方法であって、

前記情報記録媒体の記憶領域に格納されているパケットデータ単位に暗号化された所定情報を読み出す読出工程と、

前記読出工程で読み出した前記所定情報を、パケットデータ単位に異なる複数の鍵情報を用いてそれぞれ復号化することにより再生する再生工程と、

を具備することを特徴とする情報再生方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、パケットデータを扱う情報記録再生装置であって、特にパケットデータを暗号化し復号化する情報記録再生装置及び情報記録媒体とその方法に関するものである。

【0002】

【従来の技術】最近、デジタル情報を扱う情報記録再生装置の普及が進むに従って、著作物保護の観点から第三者の不正な複写処理への対策が要望されている。例えば、DVDビデオレコーディング (DVD Video Recording) 規格に対し暗号化を適用する際には、記録機器・記憶媒体・記録するデータの一部(8バイト)から生成される鍵を用いて、MPEGプログラムストリーム (MPEG Program Stream) 準拠のパック単位でデータの暗号化を行う。

【0003】すなわち、DVDビデオレコーディング規格では、記録機器・記憶媒体から得られる情報をもとに鍵を生成し、これを記憶媒体に記録しており、記録機器は、2048バイトのMPEGプログラムストリーム準拠のパックを生成し、このうちの8バイトとコピーコントロール情報と前述の鍵とを組み合わせる新たな鍵を生成し、この鍵をもとに2048バイトのうちの1920バイトのデータの暗号化を行っている。

【0004】

【発明が解決しようとする課題】しかしながら、DVDストリームレコーディング (DVD Stream Recording) 規格に前述の方法を適用して、MPEGプログラムストリーム準拠のパックを暗号化すると、アクセスに必要な時間情報等も暗号化されてしまうので、これらの情報へのアクセスが行いにくくなるという問題がある。

【0005】又更に、第三者の不正な解読に対して、解読の困難性を高めるための余地を残しているという問題がある。

【0006】本発明は、上記問題に鑑み、パケットごとに異なる鍵情報で暗号化を行うことにより、高い解読困難性とアクセスの高速化を可能とする情報記録再生装置を提供することを目的としている。

【0007】

【課題を解決するための手段】本発明は、上記目的を解決すべく、情報記録媒体に所定情報を記録する情報記録装置であって、パケットデータを単位として与えられる複数のパケットデータである所定情報を入力する入力

手段と、前記入力手段が入力した所定情報を、パケットデータごとに異なる複数の鍵情報を用いてそれぞれ暗号化する暗号化手段と、前記暗号化手段により暗号化された暗号化所定情報を、前記情報記録媒体の記憶領域に記録する記録手段とを具備することを特徴とする情報記録装置である。

【0008】本発明は上述した構成により、複数のパケットデータからなる所定情報を暗号化して例えば光ディスク等の情報記録媒体に記録する場合に、パケットデータごとに異なる鍵情報、一例として、そのパケットが情報記録装置のインタフェース等の入力手段に到着した時間情報 (arrival time) 等を鍵情報として、時間情報以外の情報を暗号化して、情報記録媒体に記録するものである。これにより、不正な複写を行おうとする第三者は、解読するための鍵情報が多く、従来に比べ解読が非常に困難になるため、高いセキュリティを可能とする情報記録装置を提供することができる。

【0009】又本発明は、情報記録媒体に格納されている所定情報を再生する情報再生装置であって、前記情報記録媒体の記憶領域に格納されているパケットデータ単位に暗号化された所定情報を読み出す読出手段と、前記読出手段が読み出した前記所定情報を、パケットデータ単位に異なる複数の鍵情報を用いて復号化することにより再生する再生手段とを具備することを特徴とする情報再生装置である。

【0010】本発明は上述した構成により、情報記録装置の場合と同様に、情報記録媒体の記憶領域に格納しているパケットデータを、パケットデータ毎に異なる鍵情報により暗号化した複数のパケットデータによる所定情報を再生するものである。従って、従来装置に比べ一層、暗号の解読困難性を向上させることができる情報再生装置を提供することが可能となる。

【0011】

【発明の実施の形態】以下、図面を参照しながら本実施例を説明する。

【0012】＜第1の実施形態＞第1実施形態は、パケットデータ毎に異なる鍵情報を用いてパケットデータの暗号化を行う情報記録再生装置、情報記録媒体及びこの方法を提供するものであり、特に鍵情報を、到着情報とパケットデータの一部とに基づいて生成する場合を詳細に述べている。図1は、本発明に係るパケットデータを記録再生するシステムの一例を示すシステム図、図2は、DVD-SR規格にてパケットを記録したときのデータ構造を示す図、図3は、本発明に係る情報記録再生装置の記録機能の一例を説明するための説明図、図4は、再生機能の一例を説明するための説明図。図5は、記録機能の一例を説明するためのフローチャート、図6は、再生機能の一例を説明するためのフローチャートである。又更に、図7は、記録機能の一例を説明するための説明図、図8は、再生機能の一例を説明するための説

明図、図9は、情報記録再生装置の暗号化の工程を示す説明図、図10は、情報記録再生装置の復号化の工程を示す説明図、図13は、情報記憶媒体の管理情報の構造の一例を示す図、図14は、情報記憶媒体のオブジェクト情報の構造の一例を示す図である。

【0013】本発明に係る情報記録再生装置Aは、図1において、パケットデータを記録再生する情報処理システムを示しており、衛星デジタル放送から配信させるパケットデータ(例えばMPEG-TS:MPEG Transport Streamの場合、188バイトのデータ)は、受信機Rを通して、セットトップボックス(Set Top Box(以下、STBと呼ぶ))Sで受信される。セットトップボックスSは例えばチューナ部1とMPEGプロセッサ部2等を有している。受信したパケットデータはIEEE1394インタフェースといったデジタルインタフェースを通して、本発明の対象となる情報記録再生装置Aに送られる。情報記録再生装置Aは、送られてきたパケットデータのパケット1つ1つに対して時間情報を割り振り、パケットデータをこの時間情報とともに情報記憶媒体に記録する。

【0014】又、再生に関しては、情報記録再生装置Aが情報記憶媒体Dから時間情報とパケットを読み出し、この時間情報に従ってパケットをSTB(S)にデジタルインタフェースを通して送られる。STB(S)は、アナログテレビに対しては、MPEGデコードを行いアナログ信号に変換して、デジタルテレビTに対してはパケットをそのままの状態で転送する。

【0015】DVD-RAM、DVD-RW、DVD-R等といった情報記憶媒体に前述のパケットを記録する場合、DVDフォーラムにおいて議論されているDVDストリームレコーディング(DVD-SR)規格が適用される。

【0016】図2には、DVD-SR規格にてパケットを記録したときのデータ構造を示す。DVD-SR規格では、受信したパケット(MPEG-TSの場合188バイト)とその時間情報(4バイト)を交互に記録し、MPEGプログラムストリーム準拠のパック(2048バイト)を構成する。2048バイトのMPEG-PSパックは32個、つまり64kBを編集の単位とする(SOB)。一番組を表すSOBは一個以上のSOBUから構成され、DVD-SRのオブジェクトデータはこのSOBが一つ以上で構成されている。情報記録媒体にはこのオブジェクトデータと、オブジェクトデータの再生順序の情報等を含む管理情報を記録する。

【0017】(記録処理)図3には本発明で提案するパケットデータを暗号化し、情報記憶媒体で記録する機器の例を示す。記録機器A1は、パケットとコピーコントロール情報をデジタルインタフェースを通して受け取るためのデータ入力部65と、パケットの到着した時間を計測するタイムカウンタ部13と、パケットをパケッ

ト、コピーコントロール情報、時間情報、機器情報、情報記憶媒体の情報(ディスク情報)を用いて暗号化するための暗号化器11と、暗号化されたパケット、コピーコントロール情報、時間情報を情報記憶媒体のフォーマットに変換するフォーマッタ部12と、変換されたデータを記録するための情報記憶媒体Dとを有する。

【0018】図5はデジタルインタフェースからパケットを受け取り、暗号化して、情報記憶媒体に記録するまでの大まかな流れを示すフローチャートである。このフローチャートにおいて、情報記録再生装置Aは、デジタルインタフェースのデータ入力部65から記録するパケットとそのコピーコントロール情報を受け取る(S11)。また同時に、記録機器A1はパケット1つ1つが機器に到着した時間をタイムカウンタ部13で計測し、その時間情報をパケットごとに生成する(S12)。

【0019】コピーコントロール情報には、例えば、“コピー禁止”、“コピー1回可(暗号化必要あり)”、“コピー可(暗号化必要あり)”、“コピー可(暗号化必要なし)”といった情報が含まれており、記録機器はその情報に従う(S13)。例えば“コピー禁止”の場合は記録機器は記録動作自体を行わないが、“コピー1回可(暗号化必要あり)”の場合は(S14)、パケットの暗号化を行う(S15)。更にコピーコントロール情報を“コピー禁止”に変更し、“コピー可(暗号化の必要あり)”ならパケットの暗号化のみを行い(S15)、“コピー可(暗号化の必要なし)”ならパケットの暗号化を行わない。暗号化は、パケットの一部、コピーコントロール情報、パケットの到着した時間に関する情報(時間情報)、記録機器の情報、情報記憶媒体の情報(ディスク情報)を用いて、パケットごとに対して、暗号化器11において行う。

【0020】更に、フォーマッタ部12において、暗号化されたパケット、コピーコントロール情報、時間情報を情報記憶媒体の記録形式に変換する(S16)。最後に、この記録データを記録部において、情報記憶媒体Dに記録する(S17)。

【0021】(再生処理)図4には本発明で提案する、情報記憶媒体より読み出したパケットデータを復号する再生機器A2の例を示す。再生機器A2は、情報記憶媒体に記録されているデータを読み出す再生部と、読み出されたデータからパケットとコピーコントロール情報と時間情報を抽出するデコード部22と、暗号化されたパケットをパケットの一部、コピーコントロール情報、時間情報、機器情報、情報記憶媒体の情報(ディスク情報)を用いて復号化するための復号化器21と、時間情報に合わせて復号化されたパケットを転送するためのタイミングカウンタ部13と、パケットとコピーコントロール情報をデジタルインタフェースを通して転送するためのデータ出力部65とを有する。

【0022】図6はパケットを情報記憶媒体から読み出

し、復号化して、デジタルインタフェースに転送するまでの大まかな流れを示すフローチャートである。図6のフローチャートにおいて、再生機器A2は、再生部において、情報記憶媒体から記録されている再生データを読み出す(S21)。デコード部では、読み出されたデータから、パケット、コピーコントロール情報、時間情報をそれぞれ抽出する(S22)。コピーコントロール情報には、例えば、“コピー禁止”、“コピー可(暗号化必要あり)”、“コピー可(暗号化必要なし)”といった情報が含まれており、再生機器はその情報に従って、“コピー禁止”や“コピー可(暗号化必要あり)”なら(S23)、復号化器にて復号化を行い(S24)、“コピー可(暗号化必要なし)”ならデータはそのままの状態転送する(S25)。更に、時間情報はタイミングカウンタ部13に送られ(S26)、復号化器21から読み出されたパケットはタイミングカウンタ部13の時間情報に従って、データ出力部65からデジタルインタフェースを通して外部に出力される。

【0023】(暗号化器) 図7に本発明で用いる暗号化器11の概要を示す。暗号化に必要な鍵は、情報記憶媒体に記録されているディスク情報、記録機器に記録されている機器情報、コピーコントロール情報、パケットの一部、時間情報を用いて生成する。鍵の一部にパケットの一部や時間情報を用いることにより、パケットごとに異なる鍵で暗号化が可能であり、この暗号を解読することが難しくなる。また、暗号化は、鍵の生成に用いた部分以外のパケットに対してのみ行い、時間情報が暗号化されることはない。これにより時間情報に直ちにアクセスすることが可能となる。

【0024】(復号化器) 図8に本発明で用いる復号化器の概要を示す。図7で示したように、鍵の生成には、情報記憶媒体に記録されているディスク情報、再生機器に記録されている機器情報、コピーコントロール情報、パケットの一部、時間情報を用いる。つまり、暗号化したときに生成した鍵と全く同じ鍵を復号化のために生成する。この鍵を用いて、パケットの暗号化された部分を復号する。復号化されたパケット部分は、鍵として用いられたパケット部分と併せることにより、もとのパケットに戻すことができる。

【0025】(暗号化の工程) 図9はパケットを暗号化する流れの一例を示す説明図である。タイトルキーとは、情報記憶媒体に記録されているディスク情報と、情報記録再生装置に記録されている機器情報から生成される7バイトの鍵であり、暗号化されて8バイトの暗号化タイトルキーとして、情報記憶媒体に記録されている。このタイトルキーは情報記憶媒体固有の鍵であり、かつ、この情報記憶媒体Dを用いる限りは共通の鍵である。この暗号化タイトルキーを復号処理して、タイトルキーを得る(S41)。

【0026】更に、このタイトルキーに対し、コピーコ

ントロール情報2ビットを加算し(S42)、新たな7バイトの鍵を生成する。鍵の生成にコピーコントロール情報を含めることにより、コピーコントロール情報のみを改ざんすることに意味がなくなる。例えば“コピー禁止”の属性をもつパケットのコピーコントロール情報を“コピー可(暗号化必要あり)”のコピーコントロール情報に変えたとしても、復号化するときと暗号化したときの鍵が異なってくるため、復号ができなくなる。

【0027】次に、4バイトの時間情報とパケットの一部の4バイト(図中ではパケットB)を併せた計8バイトのデータと前述の7バイトの鍵から、更に新たな7バイトの鍵を生成する(S43)。時間情報はパケットごとに異なるため、生成された鍵はパケット固有の鍵となる。この鍵を用いて、残りのパケット(図中ではパケットA)の暗号化を行う(S44)。

【0028】例えばMPEG-TSパケット188バイトを暗号化する場合、鍵に使う4バイトの部分をMPEG-TSのヘッダ部分とすることにより、残り184バイトが暗号化され、ヘッダ部分4バイトが暗号化されないため、たとえMPEG-TSパケットが暗号化されても、そのパケットの属性をヘッダ部分から読みとることができる。

【0029】最後に、鍵の生成に用いた4バイトのパケット部分(パケットB)と残りの暗号化されたパケット部分(図中では暗号化パケットA)を併せ(併せたものを暗号化パケットと呼ぶ)、時間情報、コピーコントロール情報とともに、情報記憶媒体に記録する。

【0030】(復号化の工程) 図10は、図9のように暗号化されたパケットを復号する流れの一例を示す説明図である。まず、情報記憶媒体から8バイトの暗号化されたタイトルキーを読み出し、復号化処理を施して7バイトのタイトルキーを生成する(S51)。次に、このタイトルキーに情報記憶媒体から読み出したコピーコントロール情報2ビットを加算し(S52)、新たな7バイトの鍵を生成する。更に、これも情報記憶媒体から読み出した4バイトの時間情報とパケットの一部である4バイト(図中ではパケットB)を併せた計8バイトのデータと、前述の7バイトの鍵から、新たな7バイトの鍵を生成する(S53)。これら一連のプロセスは前述のパケットを暗号化する際の鍵を生成するプロセスと同じものである。つまり、復号するための鍵は暗号化したときの鍵と全く同じものとなる。

【0031】例えば、図9のように記録されたMPEG-TSの場合、情報記憶媒体には4バイトの時間情報、4バイトの暗号化されていないパケットの一部(パケットB)、184バイトの暗号化されたパケットの一部(暗号化パケットA)が記録されている。この184バイトの暗号化されたパケットを前述の7バイトの鍵を用いて復号する。復号化された184バイトのパケットの一部(パケットA)は4バイトのパケットの一部(パケットB)

と併せることにより、もとの188バイトのMPEG-TSパケットに復号化する(S54)。

【0032】(管理情報)図13において、本発明に係る情報記憶媒体である、書き換え可能なディスク形状の情報記憶媒体D内のユーザが情報を記録できる領域であるData Area112内には、一般コンピュータ情報記録領域120とストリーム・データ関連情報記録領域121が混在できるフォーマットになっている。

【0033】本発明の実施形態において、記録可能なパケットデータはオブジェクトと呼ばれ、Stream Object記録領域131内に記録され、そのオブジェクトに関連する情報は管理情報記録領域130内に記録される。またアプリケーション管理情報記録領域132には本発明における情報記録再生装置に接続されているSTB等の情報が記録されている。

【0034】管理情報記録領域130は、記録したオブジェクトの管理情報が記録されているRTR Stream Manager Information (RTR SMGI) 140、記録したオブジェクトの属性情報が記録されているStream File Information Table (SFIT) 141、再生情報が記録されているOriginal PGC Information (ORG PGC) 142、プレイリスト情報が記録されているUser Defined PGC Information Table (UD PGCIT) 143、テキスト情報が記録されているText Data Manager (TXDT MG) 144から構成される。

【0035】またRTR Stream Manager Information (RTR SMGI) 140はオブジェクトの管理情報が記録されているSMGI Management Table (SMGI MAT) 150とプレイリスト情報が記録されているPlay List Search Pointer Table (PL SRPT) 151から構成され、本発明の実施形態における暗号化されたタイトルキーはSMGI Management Table (SMGI MAT) 150内のEncrypted Title Key Information (ETKI) 160に記録される。

【0036】(オブジェクト情報)図14には情報記憶媒体のオブジェクト情報の構造例を示す。本発明の実施形態においては、前述のようにパケットデータはStream ObjectとしてStream Object記録領域131内に記録される。Stream Object記録領域131には、2048バイトのMPEGプログラムストリーム準拠のStream Pack (S PCK) 170が記録される。このStream Pack (S PCK) 170は、Pack Header180、PES Header181、Sub Stream ID182、Application Header183、Application Header Extension184、Application Packet Area185で構成される。

【0037】Application Header183は、EXTENSION_HEADER_INFO190、ENCR_FLG191等から構成される。EXTENSION_HEADER_INFO190は、Application Header Extension184の領域を確保するか否かの情報であり、コピーコントロール情報を記録する場合は、Appl

ication Header Extension184の領域の確保を意味する“10b”か“11b”をセットする。ENCR_FLG191は、Stream Pack (S PCK) 170内に暗号化されているパケットを含むか否かを示す情報である。このStream Pack (S PCK) 170に、パケットの暗号化を意味するコピーコントロール情報を1つ以上含むなら、“1b”(Stream Pack (S PCK) 170内に暗号化パケットを含む、を意味する)をセットする。

【0038】Application Header Extension184には、Stream Pack (S PCK) 170に含まれているパケットの個数分のコピーコントロール情報192が含まれている。コピーコントロール情報192はStream Pack (S PCK) 170内のパケットと一対一に対応しており、例えば“00b”の場合“コピー可(暗号化必要なし)”、“11b”の場合“コピー禁止”、“10b”の場合“コピー可(暗号化必要あり)”等の値がコピーコントロール情報192にセットされる。

【0039】Application Packet Area185はパケットの到着した時間を示す時間情報193と暗号化パケット194で構成されている。時間情報193と暗号化パケット194も一対一に対応しており、時間情報193、暗号化パケット194、時間情報193、暗号化パケット194...のように交互に記録されている。

【0040】以上本発明によれば、複数のパケットからなる所定情報を、パケット毎に異なる鍵情報、例えば、パケットの到着時間やパケットのヘッダを用いることにより、第三者の解読を著しく困難にし、更に時間情報は暗号化することなく情報記憶媒体に格納されるので、時間情報を用いて情報にアクセスした場合に迅速な処理を可能とするものである。

【0041】<第2の実施形態>第2実施形態は、パケットデータ毎に異なる鍵情報を用いてパケットデータの暗号化を行う情報記録再生装置、情報記録媒体及びこの方法を提供するものであり、特に鍵情報を、パケットデータに含まれるヘッダ(又はこの一部)を用いることを特徴とする。図11は、本発明に係る第2の実施形態である情報記録再生装置の暗号化の工程を示す説明図、図12は、本発明に係る第2の実施形態である情報記録再生装置の復号化の工程を示す説明図である。

【0042】(暗号化の工程)図11は、本発明に係る第2の実施形態である情報記録再生装置の暗号化の工程を示す説明図であり、ここでは図9とは異なり、時間情報は用いず、パケットの一部のみを用いて鍵を生成する。また、暗号化手法の制約等の理由で暗号化をしないパケット部分が存在する。

【0043】まず、情報記録再生装置は情報記憶媒体のRTR Stream Manager Information (RTR SMGI) に記録されている暗号化タイトルキーを読み出し、これを復号してタイトルキーとする(S41)。更に、このタイトルキーに対し、コピーコントロール情報2ビット

を加算し(S42)、新たな7バイトの鍵を生成する(S43)。以上の処理は図9の鍵の生成処理と全く同じものである。

【0044】例えば、MPEG-TSパケット188バイトを暗号化する場合、パケットのうち8バイト(図中ではパケットB、これは一例としてヘッダである)を鍵の一部として用い、前述の7バイトの鍵から新たな7バイトの鍵を生成する。残りのパケット部分のうち176バイト(図中ではパケットA)を、この鍵を用いて暗号化を行う(暗号化パケットA)(S44)。更に残りの4バイトのパケット部分(図中ではパケットC)は暗号化もされず、鍵の一部ともならないパケット部分である。

【0045】最後に、時間情報と、鍵の一部であるパケット部分(パケットB)と暗号化されたパケット部分(暗号化パケットA)とそれ以外のパケット部分(パケットC)を暗号化パケットとして、情報記憶媒体に記録する。

【0046】(復号化の工程)図12は、本発明に係る第2の実施形態である情報記録再生装置の復号化の工程を示す説明図であり、図11のように暗号化されたパケットを復号する流れの一例を示す。まず、情報記憶媒体から8バイトの暗号化されたタイトルキー読み出し、復号化処理を施し復号化処理して7バイトのタイトルキーを生成する(S51)。次に、このタイトルキーに情報記憶媒体から読み出したコピーコントロール情報2ビットを加算し、7バイトの鍵を生成する(S52)。更に、暗号化する場合に鍵の一部としたはずの8バイトのパケット部分(パケットB)を用いて、新たな7バイトの鍵を生成する(S53)。この復号のための鍵は暗号化の際に生成した鍵と全く同じものとなる。

【0047】例えば、図11のように記録されたMPEG-TSの場合、情報記憶媒体には4バイトの時間情報、8バイトの鍵の一部となっているパケット部分(パケットB)、176バイトの暗号化されたパケット部分(暗号化パケットA)、4バイトの暗号化されず鍵の一部ともなっていない部分(パケットC)が記録されている。暗号化された176バイトのパケット部分(暗号化パケットA)は、前述の7バイトの鍵を用いて復号化される。復号化された176バイトのパケット部分(パケットA)は、鍵の一部となっているパケット部分(パケットB)とそれ以外のパケット部分(パケットC)とを併せることにより、もとの188バイトのMPEG-TSパケットに復元することができる。

【0048】以上、本発明の第2実施形態によれば、パケットデータの暗号化、復号化を行う際の鍵情報を、第1実施形態とは異なって時間情報を参考とせず、例えばヘッダ情報であるパケットBを用いて生成するものであり、これにより、第三者の解読を著しく困難にし、更に時間情報は暗号化することなく情報記憶媒体に格納されるので、時間情報を用いて情報にアクセスした場合に迅

速な処理を可能とするものである。

【0049】<第3の実施形態>第3実施形態は、パケットデータ毎に異なる鍵情報を用いてパケットデータの暗号化を行う情報記録再生装置、情報記録媒体及びこの方法を提供するものであり、特に鍵情報を、到着時間である時間情報とパケットデータのペイロード(の一部)とに基づいて生成する場合を詳細に述べている。図15は、本発明に係る第3の実施形態である情報記録再生装置の暗号化の工程を示す説明図、図16は、復号化の工程を示す説明図、図17は本発明に係る光ディスク情報記録再生装置の一例を示すブロック図である。

【0050】(暗号化の工程)図15において、第3の実施形態である情報記録再生装置の暗号化の工程を示すが、ここでは図9とは異なり、パケットが暗号化されるパケット、鍵の一部となるパケット、暗号化されないパケットの3つが存在する。

【0051】まず、情報記録再生装置は情報記憶媒体のRTR Stream Manager Information(RTR SMGI)に記録されている暗号化タイトルキーを読み出し、これを復号してタイトルキーとする(S41)。更に、このタイトルキーに対し、コピーコントロール情報2ビットを加算し、新たな7バイトの鍵を生成する(S42)。なお、以上の処理は図9の鍵の生成処理と全く同じものである。

【0052】例えば、MPEG-TSパケット188バイトを暗号化する場合、4バイトの時間情報とパケットのうち4バイト(これはヘッダ部分以外の4バイトとする、図中ではパケットC)を鍵の一部として用い、前述の7バイトの鍵から新たな7バイトの鍵を生成する(S43)。残りのパケット部分のうちMPEG-TSヘッダ4バイトを含む8バイトは暗号化を行わない部分とし(図中ではパケットB)、残りの176バイト(図中ではパケットA)に対して、前述の鍵を用いて暗号化を行う(S44)。MPEG-TSヘッダには、そのパケットの属性情報が含まれているため、そのパケットへのアクセスを容易にするためにも暗号化しないことがのぞましい。また、暗号化単位が8バイトである場合、この例においては暗号化できない部分が4バイト発生する。結果的に8バイトの暗号化しない部分が存在する。

【0053】最後に、時間情報と、鍵の一部であるパケット部分(パケットC)と暗号化されたパケット部分(暗号化パケットA)とヘッダ部分を含むそれ以外のパケット部分(パケットB)を暗号化パケットとして、情報記憶媒体に記録する。

【0054】(復号化の工程)図16は復号化の工程を示す説明図であり、この図において、まず、情報記憶媒体から8バイトの暗号化されたタイトルキー読み出し、復号化処理を施し7バイトのタイトルキーを生成する(S51)。次に、このタイトルキーに情報記憶媒体から読み出したコピーコントロール情報2ビットを加算

し、7バイトの鍵を生成する(S52)。更に、パケットの時間情報4バイトと暗号化したときに鍵の一部としたはずの4バイトのパケット部分(パケットC)を用いて、新たな7バイトの鍵を生成する(S53)。この復号のための鍵は暗号化の際に生成した鍵と全く同じものとなる。

【0055】例えば、図15のように記録されたMPEG-TSの場合、情報記憶媒体には4バイトの時間情報、4バイトの鍵の一部となっているパケット部分(パケットC)、176バイトの暗号化されたパケット部分(暗号化パケットA)、ヘッダ部分を含む8バイトの暗号化されず鍵の一部ともなっていない部分(パケットC)が記録されている。暗号化された176バイトのパケット部分(暗号化パケットA)は、前述の7バイトの鍵を用いて復号化される(S54)。復号化された176バイトのパケット部分(パケットA)は、鍵の一部となっているパケット部分(パケットC)とそれ以外のパケット部分(パケットB)と併せることにより、もとの188バイトのMPEG-TSパケットに復元することができる。

【0056】以上本発明の第3実施形態によれば、パケットデータの暗号化、復号化を行う際の鍵情報を、パケットの到着時間である時間情報とペイロード部分(ヘッダ以外のパケットの情報)の一部とを用いて生成するものであり、これにより、第三者の解読を著しく困難にし、更に時間情報は暗号化することなく情報記憶媒体に格納されるので、時間情報を用いて情報にアクセスした場合に迅速な処理を可能とするものである。

【0057】<本発明に係る光ディスク記録再生装置の実施形態>次に上述した情報記録再生装置の処理を行う具体的な一例として、光ディスク記録再生装置を詳細に説明する。図17において、上述した本発明に係る暗号化復号化処理を行う光ディスク記録再生装置の一例のブロック図が示される。

【0058】図3において、システム制御部62はRAM61を作業エリアとして使用し、ROM60に記録された本発明を含むプログラムに従って所定の動作を行う。光ピックアップ54から出力された光は、光ディスクDに照射される。光ディスクDからの反射光は、ヘッドアンプで電気信号に変えられる。この電気信号は、信号処理部56に入力される。信号処理部56には、RFアンプなどが含まれる。

【0059】又サーボ制御系各処理回路55には、上述した対物レンズ誘導回路21やフォーカス制御回路22、対物レンズ駆動信号切替器24、対物レンズ駆動回路やウォブル(WB)信号検出部等が含まれており、上述したように光ディスクの面ぶれを排除して安定したフォーカス引き込み動作等を行う。

【0060】この動作に併せて、ウォブル信号も検出され、これに応じて生成された書込みクロックは、読取りバッファ57に供給される。

【0061】データ書込み動作時は、データ処理部58が図示しないライトチャンネル回路で作られた書込みクロックを用いて、インタフェース65を通して送られてくるデータに誤り検出符号(EDC)やIDを付加し、サーボ安定のためのデータスクランブル処理を施し、更に誤り訂正符号(ECC)を付加し、同期信号を付加すると併せて、同期信号以外を変調し、書込みパワー制御部63に送って、対応メディアに最適なライトストラテジによって、レーザダイオード駆動回路64を通して、光ディスクDに信号を書き込む。

【0062】この時、図3等で上述された本発明に係る暗号化器11の暗号化工程が、このデータ処理部58の信号処理として行われるものであり、所定の鍵情報がパケットデータごとに生成され、これを用いて上述したパケットデータの暗号化が行われ、記録処理がなされる。

【0063】読出し時は、光ピックアップ54のヘッドアンプから読出されたRF信号は、最適イコライザを通して、読取りバッファ57とPLL回路に送られる。PLL回路で作られた読出しクロックで、読取りバッファ57にチャンネルデータが読み取られる。読み取られたデータは、データ処理部58で、同期化されシンボルデータが読出される。その後誤り訂正やデスクランブル処理が行われ、インタフェース65を通して外部に転送される。

【0064】同様に、図4等で上述された本発明にかかる復号化器21の復号化工程が、このデータ処理部58の信号処理として行われるものであり、所定の鍵情報をパケットデータごとに生成され、これを用いて上述したパケットデータの復号化が行われ、再生処理がなされることとなる。

【0065】このようにして、上述した光ディスク記録再生装置Aにより、本発明に係る暗号化復号化処理が施されるものである。

【0066】

【発明の効果】以上詳述したように本発明によれば、情報記録媒体に格納される所定情報をパケット毎に異なる鍵情報で暗号化し復号化することで、不正な第三者の解読を著しく困難にすることが可能となり、更にパケットデータの到着時間等の時間情報を参考に鍵情報を生成し、この時間情報を暗号化することなく記憶領域に記録することにより、時間情報に対するアクセスを早くすることで、処理速度の向上を図ることが可能となる情報記録再生装置及び情報記録媒体並びにこの情報記録再生方法を提供することができる。

【図面の簡単な説明】

【図1】本発明に係るパケットデータを記録再生するシステムの一例を示すシステム図。

【図2】本発明に係る情報記録再生装置の暗号復号方法によりDVD-SR規格にてパケットを記録したときのデータ構造を示す図。

【図3】本発明に係る情報記録再生装置の記録機能の一例を説明するための説明図。

【図4】本発明に係る情報記録再生装置の再生機能の一例を説明するための説明図。

【図5】本発明に係る情報記録再生装置の記録機能の一例を説明するためのフローチャート。

【図6】本発明に係る情報記録再生装置の再生機能の一例を説明するためのフローチャート。

【図7】本発明に係る情報記録再生装置の記録機能の一例を説明するための説明図。

【図8】本発明に係る情報記録再生装置の再生機能の一例を説明するための説明図。

【図9】本発明に係る第1の実施形態である情報記録再生装置の暗号化の工程を示す説明図。

【図10】本発明に係る第1の実施形態である情報記録再生装置の復号化の工程を示す説明図。

【図11】本発明に係る第2の実施形態である情報記録再生装置の暗号化の工程を示す説明図。

【図12】本発明に係る第2の実施形態である情報記録再生装置の復号化の工程を示す説明図。

【図13】情報記憶媒体の管理情報の構造の一例を示す図。

【図14】情報記憶媒体のオブジェクト情報の構造の一例を示す図。

【図15】本発明に係る第3の実施形態である情報記録再生装置の暗号化の工程を示す説明図。

【図16】本発明に係る第3の実施形態である情報記録再生装置の復号化の工程を示す説明図。

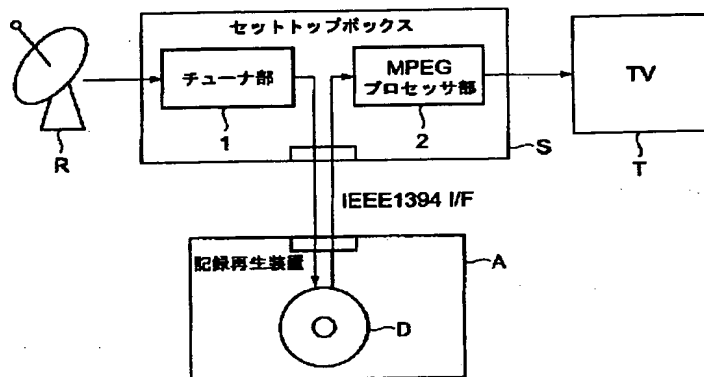
【図17】本発明に係る光ディスク情報記録再生装置の一例を示すブロック図。

【符号の説明】

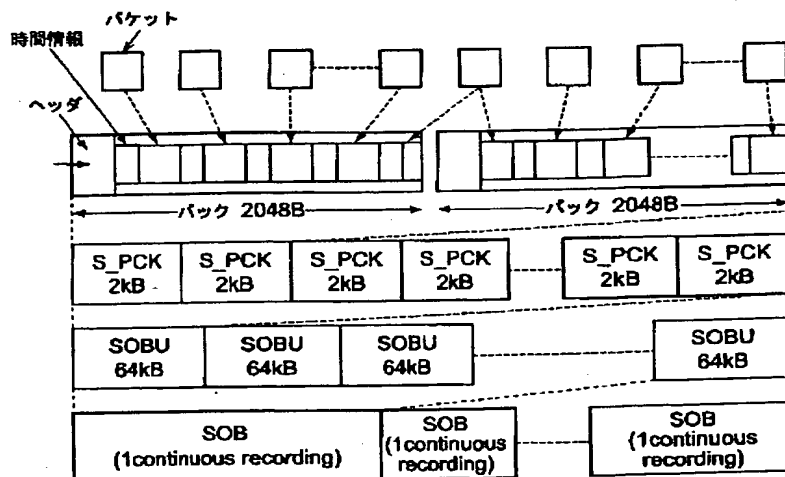
A…記録再生装置、11…暗号化器、12…フォーマッタ部

13…時間情報、14…機器情報、15…ディスク情報
21…復号化器、22…デコーダ部

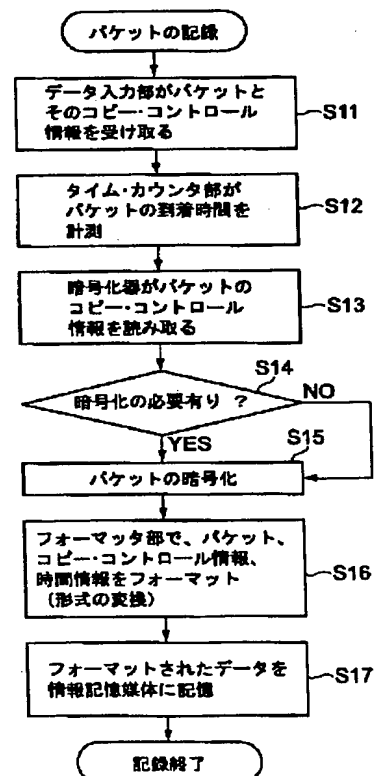
【図1】



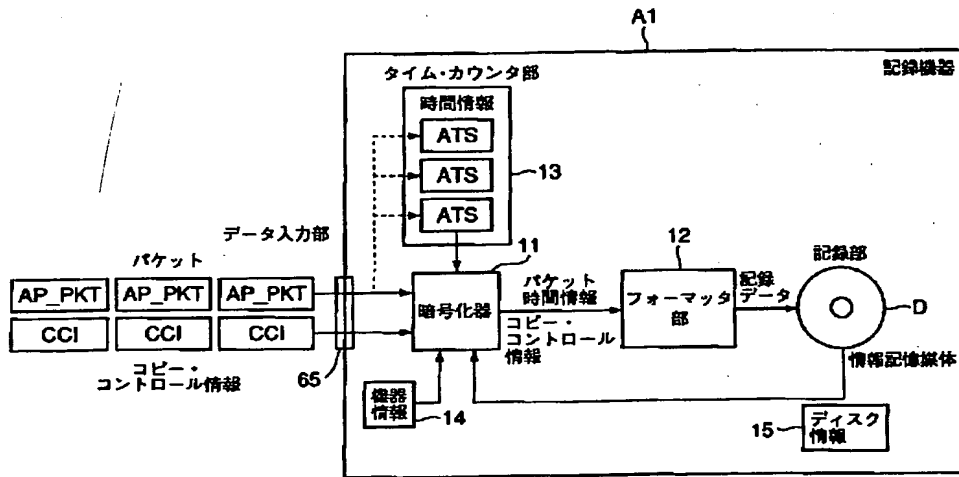
【図2】



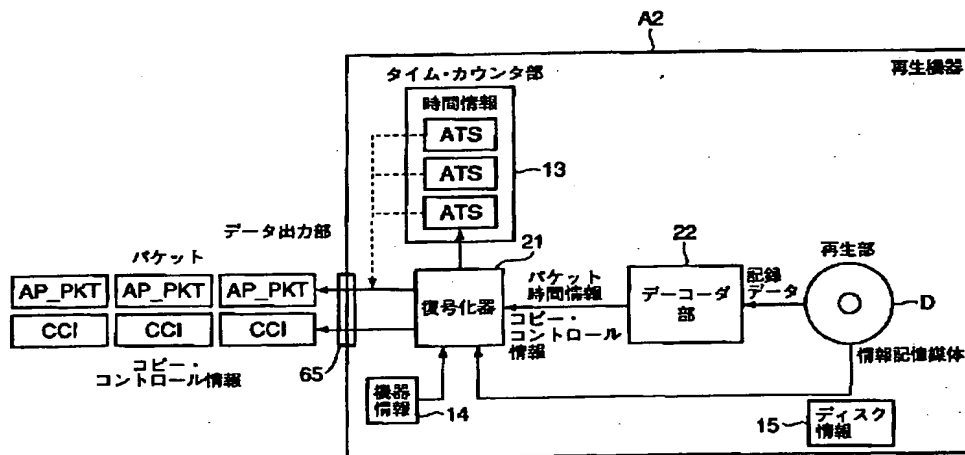
【図5】



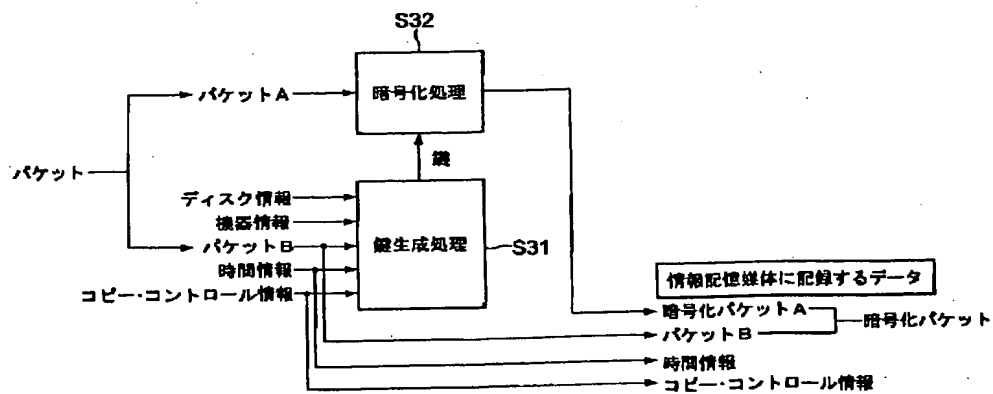
【図3】



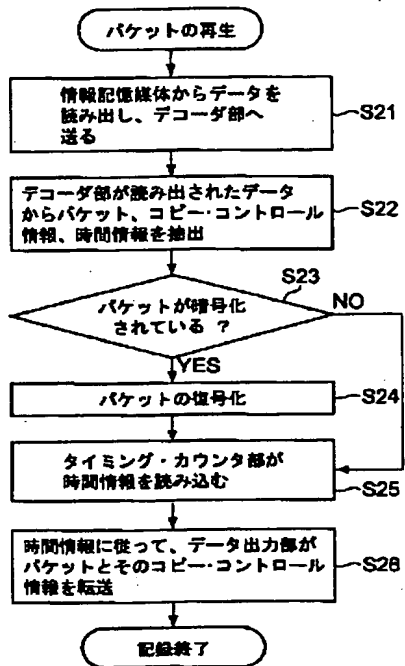
【図4】



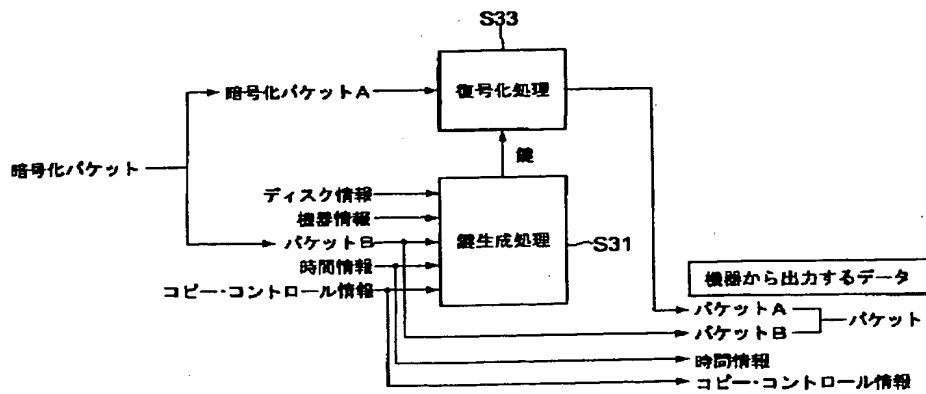
【図7】



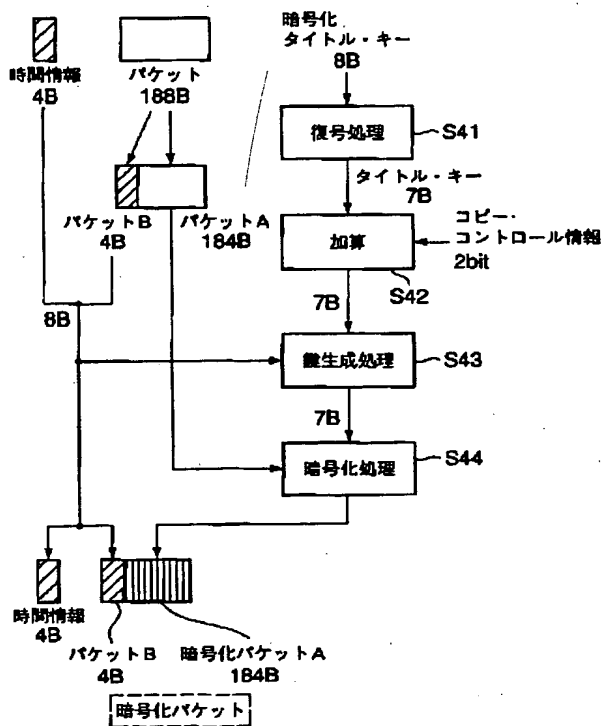
【図6】



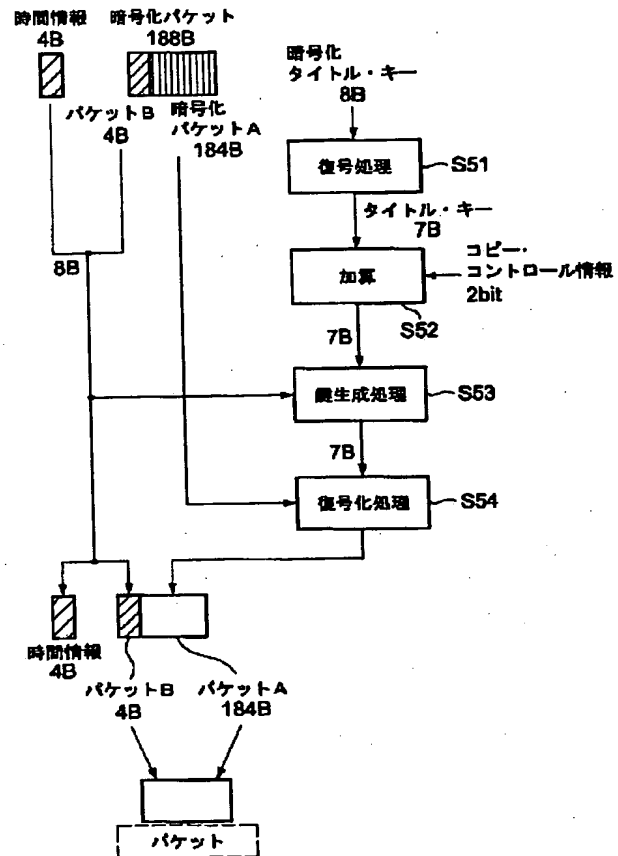
【図8】



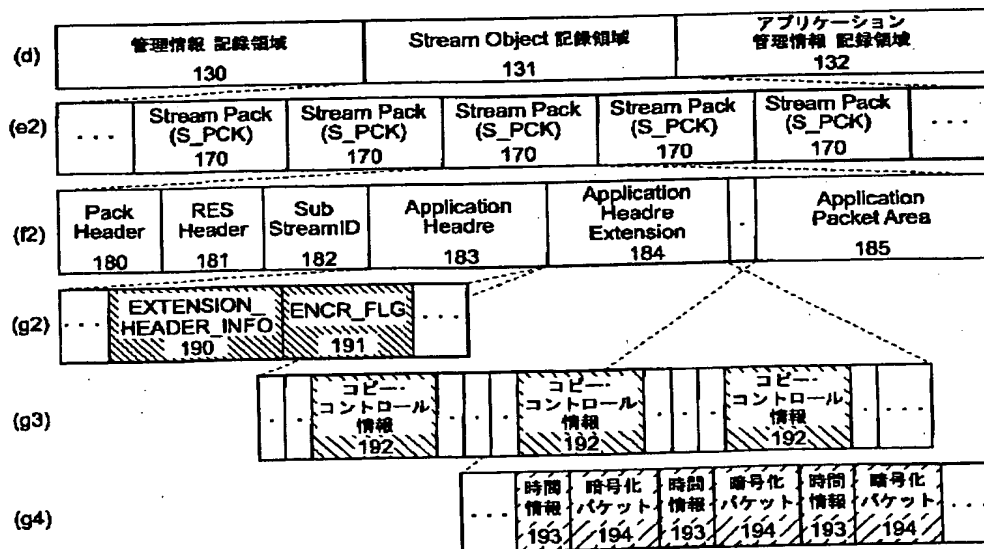
【図9】



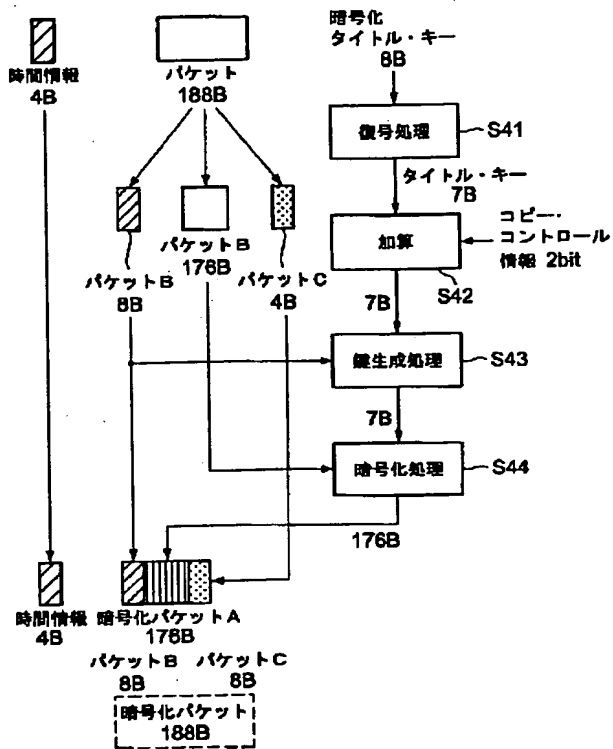
【図10】



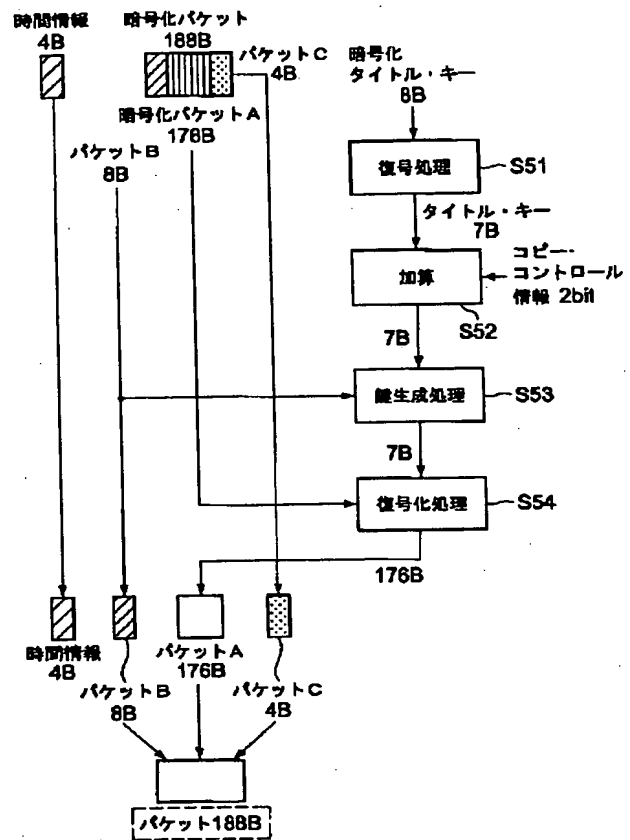
【図14】



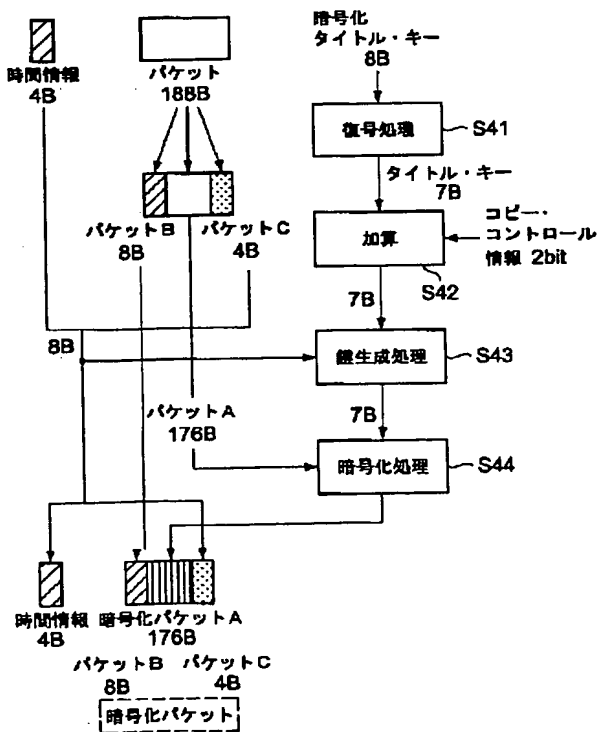
【図11】



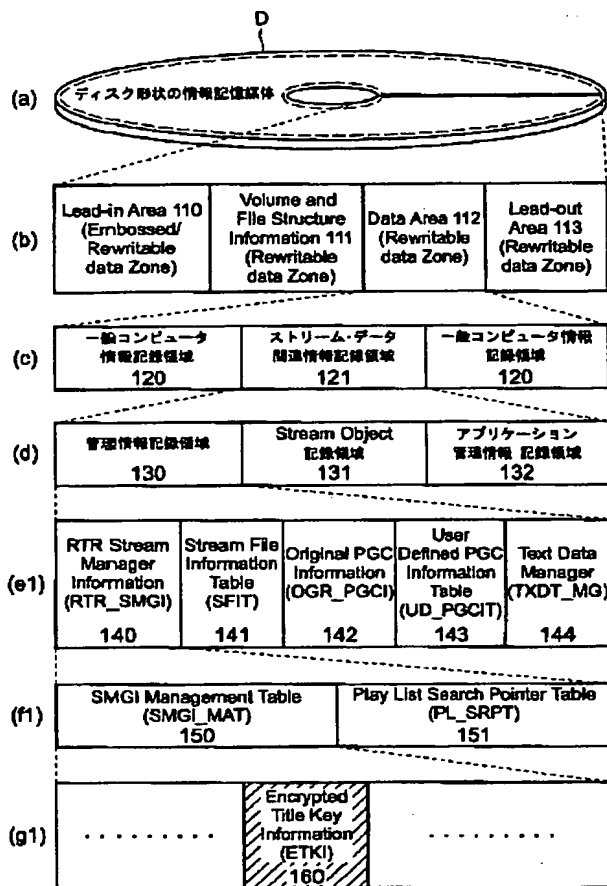
【図12】



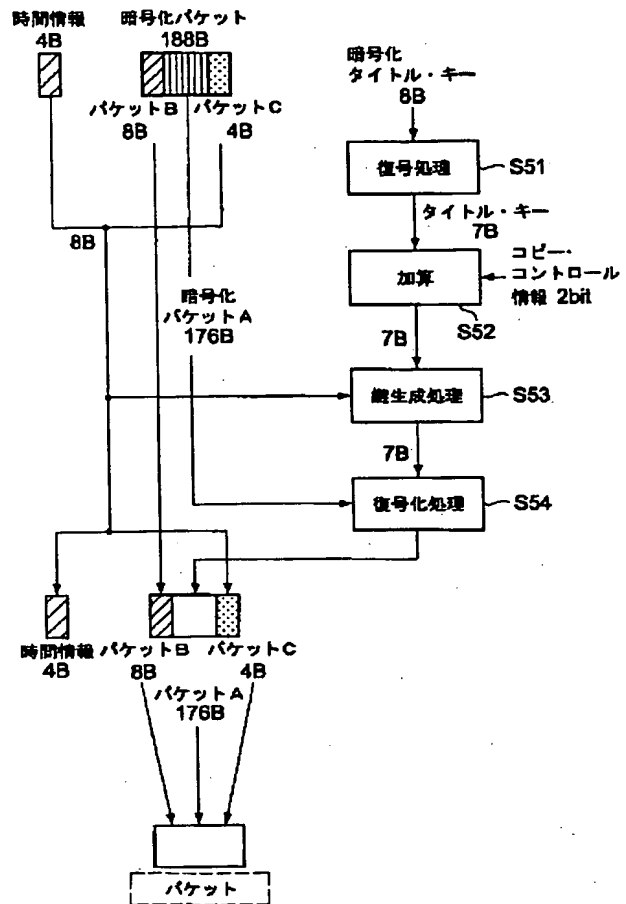
【図15】



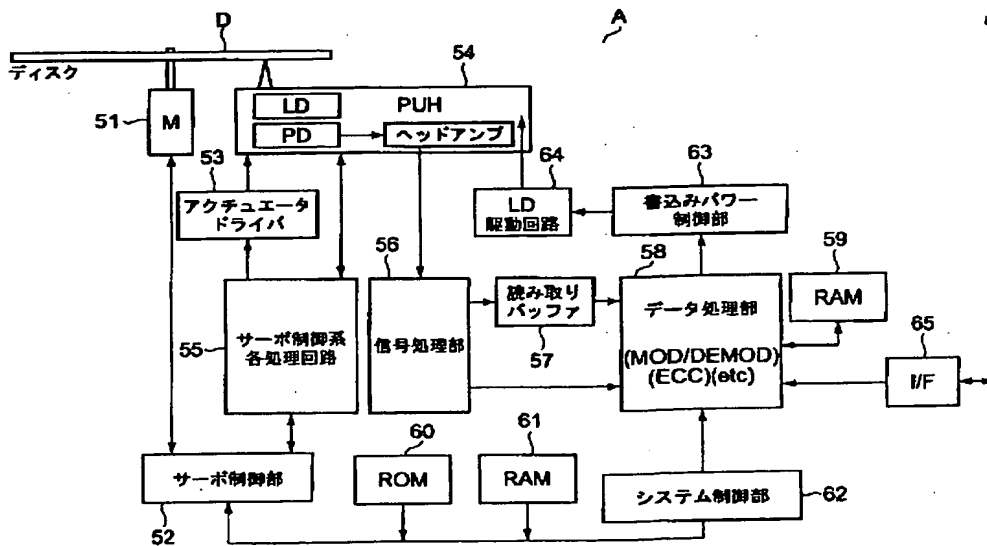
【図13】



【図16】



【図17】



フロントページの続き

(72)発明者 加藤 拓
東京都府中市東芝町1番地 株式会社東芝
府中事業所内

Fターム(参考) 5B017 AA03 BA07 CA09
5C052 AA03 AA04 AB04 CC11 CC20
DD04
5C053 FA13 FA20 FA25 GB05 GB37
GB40 JA30 LA07
5D044 AB07 BC04 CC04 DE99 GK17
5J104 AA12 AA34 NA02 NA27 PA14